STATUS OF CLAIMS:

Claims 1-6, 8-9, 11-13, 15-19, and 21 were previously canceled. Previously presented Claims 7, 10, 14, 20, and, 22-25 are active in this application.

REMARKS:

These remarks respond to the grounds of rejection set forth in the Office Action mailed on August 13, 2010. Applicants would first like to express appreciation to the Examiner for review of the Application and his findings.

Background:

Applicants note that this current Office Action does not address some of the specific arguments presented in response to the previous Office Action, with the reason stated that the arguments presented by the Applicants are moot in view of the new grounds of rejection. However, the Office Action repeats the basis of the rejection as concerns the previously cited patents such as Ilnicki and Rees. The cited portions of these references upon which reliance was placed were addressed in the last response, and thus, the same arguments are again applicable in response to the current rejection and Applicants ask that these be considered also if the present arguments are not persuasive. Without having the benefit of such arguments being addressed, Applicants are required to speculate as the why the same portions of these references are again being cited as meeting the limitations in claims 7 and 14, especially in view of the previously presented arguments. Additionally, the present Office Action is not clear as to precise grounds of rejection being given for claims 24 and 25. The first rejection recited on

page 2 of the Office Action is stated as only applying to claims 7, 10, 20 and 23 while page 5 of the Office Action of that rejection recites grounds for rejecting Claim 24. Further, claim 24 is listed on page 7 as being again rejected on different grounds but the specific grounds are given relative to claim 25. Thus, it is unclear if the first rejection should have listed claim 24 and that rejection on page 7 should refer to claim 25 and not claim 24. Applicants therefore are unable to respond to the stated grounds of rejection. In view of this and in the case this present response is not sufficient to allow for proceeding with an allowance of these claims as presented, Applicants request issuance of a further Office Action clarifying these grounds of rejection.

Applicants traverse the rejection of claims 7, 10, 20 and 23 under 35 U.S.C. 103(a) as being unpatentable over Ilnicki (6751677) in view of Subramaniam (6081900). Additionally, to the extent understood, Applicants traverse the statements in the first and second paragraphs of page 4 of the Office Action regarding the teachings of Subramaniam and the basis for incorporating such teachings into the Ilnicki system for the reasons stated herein.

Arguments:

With regards to Ilnicki, Applicants make the following arguments.

1) As previously argued, Ilnicki teaches away from providing two levels of security processing in that Ilnicki specifically teaches his invention as having the advantage of a single SSL connection for the purpose of maintaining an end to end secure sockets connection. Specifically, Ilnicki

teaches that a single level of connection is a specific advantage of his invention and thus teaches away from any approach alleged to provide two levels of security. Indeed, Ilnicki requires a single level of connection. To attempt to incorporate teachings that alter such single level of connection as suggested in the Office Action would frustrate the approach utilized in Ilnicki and prevent Ilnicki from attaining the advantages thereby obtained.

Support for this argument is provided throughout the disclosure of Ilnicki. In Ilnicki's "Summary of The Invention", the purpose of the invention is described as being "*to allow*" utilization of a single end-to-end secure connection.

Ilnicki Column 3, lines 43-48:

> *"The method also includes a step of proxifying an object reference that refers to a target server of the servers to be accessed by a user request from the user device in order to allow* ***a single end-to-end secure session*** *between the user device and the target server to be established via the gateway."*

Further support with a similar description is found in Ilnicki Column 3, lines 56-57:

> *".. the user request is not required to expose the IP address and port number of the target server and* ***the single end-to-end secure session*** *between the user device and the target server is established."*

Also, Ilnicki Column 4, lines 25-28:

> *"Once such chain of TCP/IP connection is established, the underlying client application in the user terminal establishes over these connections* ***a single SSL session*** *with the target object server."*

2) Secondly, as stated above, Ilnicki's invention could not be practiced in combination with any approach which utilizes two levels of security processing because this would be in conflict with the Ilnicki approach that utilizes a single SSL connection from end to end. That is, for the reasons stated, in Applicants' view, one skilled in the art would not attempt to incorporate into the Ilnicki system an approach that would provide for two levels of encryption because this would be in direct conflict with the principle accomplishment of Ilnicki's invention. It should also be noted that the technical background of the invention of the Subramaniam patent discusses the use of a prior art proxy server approach which is not deemed sufficiently convenient and efficient thereby further suggesting non-combination.

3) Ilnicki also presents as an advantage of his invention that the gateway / firewall is not required to "*look at*" the "*payload*" of the user request in Ilnicki Column 5 lines 39-43 "*This in turn allows secure connection to be established between the user terminal 31 and the target server of the servers 34 because the mapping is done* ***without requiring the gateway to examine or look at the encrypted payload of the user request***.".

In contrast, Applicants' invention as defined in Claim 7 includes the required step of:

> " I) the first created processes on the gateway machine handling security processing at the first security level of encryption for said messages sent and said messages received on the first port of the gateway machine, thereby removing from the server machine, security processing at the first security level of encryption for these messages.".

The "security processing at the first security level of encryption" in Applicants' claim above requires, in terms of Ilnicki, "examination" or a "look at" the "encrypted payload of the user request", which is contrary to the approach of Ilnicki that does NOT allow or permit for that "look" at the encrypted payload. That is, it is impossible to do encryption processing as defined in Applicants' claims without "looking at" the "payload" (using the terms of Ilnicki).

4) With regards to the patent to Subramaniam cited for incorporation into the Ilnicki system, it should be noted that Subramanian reference cited relative to step I also does not describe or teach any security or encryption processing being performed on a border server that serves to reduce security processing on the target server as defined in Applicants' claimed invention.

Before discussion of Subramaniam, it is very important to note that Subramaniam utilizes the **words** "secure" and "insecure" to describe a different concept than presented in Applicant's Specification. Subramaniam use of the words "secure" and "insecure" is to describe requests to data which include URLs within the data which contain "https" or "http" respectively. Subramaniam teaches "secure" to mean "transformed" (in his words) data that has had all references to URLs that are in "http" form transformed to "https" form. That is, "secure" to Subramaniam does not mean a level of "encryption" or security in viewing the data itself. Instead "secure" to Subramaniam means data including references to only "https" URLs. Subramaniam is achieving the goals of his invention by transforming URLs. In Subramaniam, encryption, decryption and other security processing such as authentication (except for redirection) are handled in a normal manner. For example, column 7, lines 25-30 cite U.S. patent no. 5,825,890 as illustrating a familiar embodiment of secure sockets layer communication.

This view is supported clearly in Subramaniam and distinctly spelled out in Subramaniam Column 9, lines 35-43 which describes clearly what is meant by the words "secure" and "non-secure", and "secure data" and "non-secure data".

> *"The **data 130 is non-secure** in that it **includes hypertext links**, URLs, or other references **which**, if presented by the external client 112 to the secure network 100, **would not necessarily require use of a secure connection such as an SSL** connection and which might allow non-secure access to protected network 100 data.*
> *For instance, **Web pages which contain URLs specifying http://** rather than https:// in reference to data stored on the target server 104 **are examples of non-secure data** 130."*

That is, Subramaniam's use of "secure" or "non-secure" (insecure) depends upon reference to any URLs contained WITHIN the data, which is not at all a reference to the encryption or security level of the data itself as in the case of Applicant's invention either as described in Applicants' Specification or as claimed.

5) Nowhere in Subramaniam is there any description of a reduction of load on the target machine, nor a description of his border server doing encryption processing for a second connection while continuing that same communication at a lower level of encryption over the first connection. Subramaniam is forcing communication with the client to utilize SSL by transforming "http://" references to the form of "https://".

When Subramaniam refers to transforming data from "insecure" to "secure", he is describing altering any URLs in the data from http to https form.

This interpretation is applicable to the FIGURES such as FIGURE 1 within Subramaniam, and even more especially to that description cited in the Office Action to Subramaniam Col. 9, lines 11-17 which reads:

> *"During a step 128, non-secure data 130 is transmitted from the target server 104 to the border server 106 where it will be modified to promote continued security and then forwarded to the external client 112 during a transmitting step 132. "*

This modification of Subramaniam to *"promote continued security"* is a description of Subramaniam's URL transformation, and is NOT a change in "security level" (of encryption) as described in Applicant's Specification or as defined in Applicants' claims. That is, the transformation does not relate to the process of data encrypting or decrypting.

Again, the modification or transformation of Subramaniam also does not achieve one main goal of Applicants' invention which is to reduce processing on the target server. Indeed, Subramaniam repeats in several places that his transformation can be done by either his border server OR on the target server, which is further evidence that he was not contemplating achieving any reduction of processing on the target server.

Subramaniam describes a "URL transformer" included within the border server OR target server which requires SSL to be utilized (after authentication), but the encryption processing required by SSL is performed in a normal manner. The approach of Subramaniam is described succinctly in Column 4 lines 11-13 as follows:

> *"the present invention forces use of HTTPS or a similar secure connection each time the user follows an URL to confidential data".*

Thus, Subramanian teaches URL **transformation** and mechanisms such as HTTP redirection and SSL software to provide secure authentication of a user from an external client and to provide secure transmission of

confidential data between the target server (identified by the user request) and the external client. By transforming non-secure URLs into secure URLs, the Subramanian invention forces continued use of secure communications despite the inherent security problems caused by the lack of state information in HTTP.

In Applicants' reading of the Subramaniam disclosure Applicants submit that SSL (decryption) software is required wherever the "transformation" of URLs is performed (either Border or Target) because in order to examine and process the URL information within the "payload" the payload must be decrypted. (Examining the data in encrypted form would not allow the URLs to be found or identified and therefore no transformation of a URL could occur). However, once this transformation to https is performed, all further communication is necessarily encrypted because that is what https requires, and this requires SSL processing on the target server.

6) Indeed, the various approaches described in Subramaniam typically require that the target server to do MORE work because in Subramaniam all URLs directed to the target server contained in an external client request are either maintained or forced (transformed) into the "https" form which is at either the same or at a HIGHER level of encryption (requiring more processing). Thus the target server of Subramaniam may indeed be required to do MORE work which is in conflict with the purpose and goals of Applicant's present invention, the main goal of Applicant's claimed present invention being to REDUCE the amount of work required to be performed by the target server. Additionally, it should be noted that when the target server contains an URL transformer, it sends secure data either directly or indirectly to the external client thereby adding to the processing burden of the target server.

7) Applicants fully agree with the Examiner's statement in the prior Final Office Action that Ilnicki does NOT describe handling of security processing at a first level with messages sent at a second level to the server machine thereby removing load of processing from the server.

Applicants submit that Subramaniam also does not describe or disclose a step or processing operation as defined and as claimed in Step F) of Applicants' Claim 7 which reads:

> *"F) establishing a second connection from the second port of the gateway machine to the first port of the server machine, the second connection to be used to exchange messages at a second security level of encryption which is reduced from the first security level of encryption;"*

This step is a prerequisite for carrying out the subsequent steps of claim 7 and more particularly step I for which Subramaniam is cited. It is pointed out in particular in this step from Applicants' Claim 7 that in Applicants' invention, the second security level of encryption is reduced from the first security level.

In contrast, Applicants' submit that a reasonable interpretation of Subramaniam is that any connection from the border server to the target server is either at the SAME level of encryption (security) OR at a HIGHER level, which as a direct result requires the same or MORE processing by the target server, not LESS. That is, **Subramaniam does not disclose or suggest** a "second connection ... at a second security level **which is** reduced from the first security level of encryption" (as claimed).

This reduction in processing by the target server is further defined in element I) of Applicants' Claim 7 by the following wording: *"thereby*

removing from the server machine, security processing at the first security level of encryption for these messages". For an "*end to end*" connection as taught in Ilnicki, this first and only security level of encryption is maintained from "end to end".

8) The major differences in arrangement and modes of operation between Ilnicki and Subramaniam would also dissuade those skilled in the art from attempting to incorporate the teachings of Subramaniam relative to a gateway/border server into the system of Ilnicki. As discussed above, Ilnicki discloses a system that includes a user terminal, a firewall having a number of ports and a gateway positioned between the firewall and a plurality of servers. By contrast, Subramaniam discloses a system that includes an external client and a secure network such as a website having a security perimeter and that includes a border server and a target server both of which can receive requests from the external client. In Ilnicki, it is of major importance that the user request is not required to expose the IP address and port number of the target server. By contrast, Subramaniam requires that the external client request identify the target by its URL. Also, the target server is required to check the IP address from which the request was made to determine if the request came from outside the security perimeter and if so redirect the request to the border server for enabling authentication to take place.

For similar reasons as stated above, Applicants traverse the rejection of claim 14 and 22 under 35 U.S.C. 103(a) as being unpatentable over Ilnicki in view of Subramaniam and in further view of Rees (6981265). Further, Applicants traverse the statements in the last paragraph of page 6 and the first two paragraphs of page 7 of the Office Action.

Conclusion:

In conclusion, Applicants submit that the boundaries and intent of the present invention are clearly defined in the presently presented Claims, and neither Ilnicki nor Subramaniam taken alone or in combination teach the invention as claimed, nor do they in combination suggest or make obvious the present claimed invention. Applicants also submit that the claims as currently presented are incorporating the proper limitations described and supported in the Specification.

Applicants further specify that the preceding arguments and discussion are for purposes of discussing one or more illustrated embodiments of Applicants' invention and should not be construed as limiting Applicants' claims. The bounds or scope of the claimed invention is as defined in Applicants' present claims as interpreted in light of the specification. If any questions should arise regarding the above arguments, amendments and this application, the Examiner is requested to call Applicants representative at the number indicated herein.

If for any reason the Examiner deems it necessary to issue a further Office Action in this application, Applicants' representative asks to be contacted prior to the issuance of such Office Action.

There have been arguments that the Office Action has not set forth for establishing a prima facie case of obviousness under 103 describing the required level of skill possessed by one skilled in the art for combining the cited patent teachings. The previous Office Action utilized Ilnicki as the main reference in combination with Vu and Rees which established one level of skill. The present Office Action utilizes Ilnicki as the main

reference in combination with Subramanian, Rees and Shimbo which is establishing a different level of skill. This, in Applicants' view potentially provides a hindsight reconstruction of Applicants' claimed invention. Utilizing combinations of previously known methods of network processing in a new way is the essence of invention in this field. If a 103 standard were to be applied which allows picking and choosing elements from other patent disclosures to establish obviousness, some of the cited patents themselves would have never been issued.

In general, the Office Action provides a conclusory rationale, without discussion or reasonable explanation of what would motivate a skilled artisan to combine Ilnicki and Subramaniam, especially considering that indeed the two inventions are directed to solving distinctively different problems and provide different approaches in solving the different problems. Furthermore, for the reasons stated above, it is not clear that a skilled artisan would have any reasonable expectation of success based upon only the prior art combination of Ilnicki and Subramaniam, or with Shimbo, especially considering the prior art from a point of view which ignores the insight and advantages potentially gained from the new teachings contained in Applicants' disclosure. (see reference In re Fine 837 F.2d 1071, and W.L. Gore, 721 F.2d at 1553, 220)

If Examiner would like to suggest Claim wording that would more clearly define the boundaries of the claims those suggestions would be welcome. Applicants sincerely thank the Examiner for his time in consideration of this application. It is believed that the Application is in form to proceed towards allowance.

Sincerely,

Russell W. Guenthner Ph.D. #54,140
Bull Enterprise Fellow

Bull HN Information Systems
13430 Black Canyon Highway
Phoenix, Arizona 85029